THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL DEFENDANT'S MOTION FOR EARLY RETURN OF TRIAL SUBPOENA TO AMAZON WEB SERVICES, INC. NOTING DATE: January 20, 2022

Pursuant to Federal Rule of Criminal Procedure 17(c) and the Sixth Amendment, defendant Paige Thompson respectfully moves this Court to enter an order permitting the early return of a trial subpoena served on Amazon Web Services, Inc. ("AWS"). AWS documents are expected to play a critical evidentiary role in Ms. Thompson's defense. In support of the motion, Ms. Thompson submits the accompanying memorandum of law, and concurrently files an *ex parte* affidavit from counsel Mohammad Ali Hamoudi *in camera* and under seal and a proposed order calling for the return of the documents no later than 7 days after the date of the order.[1] The defense

[1] Ms. Thompson files the affidavit *ex parte* and in camera because it discusses and reveals defense strategy. *See* Fed. R. Crim. P. 17(b) (permitting "a defendant's ex parte application"). In *United States v. Sleugh*, 896 F.3d 1007, 1015 (9th Cir. 2018), the Ninth Circuit recognized the need to file affidavits in support of Rule 17(c) subpoenas under seal: "Such affidavits might sketch out possible defense theories," they "are not evidence themselves," and thus, "there is no presumption of public access under the First Amendment or common law that attaches to Rule 17(c) subpoena applications and their supporting materials." *See also United States v. Fry*, 2012 WL 117117, at *1 (E.D. Wash. Jan. 13, 2012) ("[T]he *ex parte* procedure is justified in circumstances where it is necessary to avoid

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

and AWS have agreed that AWS shall have until January 14, 2022 to respond to this motion. The trial is currently scheduled for March 14, 2022.

DATED: this 4th day of January, 2022.

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI

/s/ Christopher Sanders
CHRISTOPHER SANDERS

/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

/s/ Brian Klein
BRIAN KLEIN

/s/ Melissa Meister
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

disclosure of trial strategy or a witness list[.]"); *United States v. Tomison*, 969 F. Supp. 587 (E.D. Cal. 1997) (finding a Rule 17 *ex parte* submission appropriate to protect trial strategy).

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The superseding indictment paints a picture of defendant Paige Thompson as a "hacker" who illegally obtained unauthorized access to the servers of multiple Amazon Web Services ("AWS") customers, including Capital One Bank (USA), N.A./Capital One Financial Corp.'s ("Capital One"), for nefarious purposes, and then utilized that access to copy valuable information and enrich herself by cryptojacking. The superseding indictment, however, fails to recognize that Ms. Thompson's alleged conduct has a perfectly innocent explanation: It is the same type of conduct engaged in by so-called "white hat hackers," also known as computer security experts or "researchers," who patrol the Internet looking for vulnerabilities or "misconfigurations" in servers such as the one Ms. Thompson is alleged to have accessed.

Proving criminal intent is paramount to this case, in which Ms. Thompson is charged with wire fraud, computer fraud and abuse, access device fraud, and aggravated identity theft. Although the government states in another motion that it, "will introduce evidence [Ms.] Thompson appears to have taken steps," (Dkt. 138, at 10), to obtain counterfeit credit or debit cards, Ms. Thompson has not seen—and the government has not provided the Court—any credible evidence that Ms. Thompson attempted to monetize the allegedly valuable information to which she allegedly gained access (because she did not). "Capital One is aware of no evidence that she distributed the Consumer Information in any way."[2] (Dkt. 147, at 3.)

This leaves the government grasping at two unrelated straws: (1) Ms. Thompson must have had criminal intent because after she allegedly accessed the AWS servers, she purportedly utilized their computing power to mine an insignificant amount of

[2] In the Eastern District of Virginia, Capital One represented that its personal identifying information has no independent monetary value.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

cryptocurrency; and/or (2) Ms. Thompson must have had criminal intent because she had in her possession personal identifying information (PII) that she could have monetized (though, again, there is no credible evidence that she actually did so).

The government now tells this Court that the cryptocurrency allegation is "central to the government's theory." (Dkt. 138, at 10.) But those allegations involve less than $10,000, and there is no evidence the defense has seen to demonstrate the alleged victims' servers were used for mining, or even if they were (assuming for argument's sake), that the victims bore a financial burden because of it.

The subpoena requests are meant to get at issues in dispute with the government and to assist with Ms. Thompson's defense at trial. The defense and AWS met and conferred regarding the requests and have dramatically narrowed the items in dispute. The two requests for which the defense is seeking the early return of documents and communications through this motion are directly relevant to, among other things, whether Ms. Thompson had the specific intent to commit the crimes with which she is charged, and as such, are necessary for her defense in advance of trial. These are precisely the kinds of material that Federal Rule of Criminal Procedure 17(c) permits to be returned in advance of trial, and the Court should order such here so Ms. Thompson can adequately prepare her defense—including preparing at least one expert—in advance of trial.

The Court should grant Ms. Thompson's motion.

II. RELEVANT FACTS

Ms. Thompson is charged in a ten-count superseding indictment. All of the counts relate to AWS customers, including Capital One Bank (USA), N.A./Capital One Financial Corp. ("Capital One"), and allege Ms. Thompson committed wire fraud in violation of 18 U.S.C § 1343 (Count 1), computer fraud and abuse in violation of 18

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

U.S.C. §§ 1030(a)(2)(A) and (C) and (c)(2)(A) and (B)(iii) (Counts 2-7), computer fraud and abuse in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i) (Count 8), access device fraud (Count 9), and aggravated identity theft (Count 10). (Dkt. No. 102; Aff. of Mohammad Ali Hamoudi ("Aff.") at ¶ 2.)

In general, the superseding indictment alleges Ms. Thompson "scanned" for "misconfigurations" in the "publicly facing portion" of cloud servers owned and operated by AWS but rented by the alleged victim entities. (Docket No. 102.) According to the superseding indictment, once Ms. Thompson identified such misconfigurations, she "transmitted commands to the misconfigured servers that obtained the security credentials" belonging to the victim entities. (*Id.*) Then after Ms. Thompson had these security credentials, it is alleged that she used them to obtain "lists or directories of folders or buckets of data," which she then copied to her own server; this data allegedly included "personal identifying information, from approximately 100,000,000 customers who had applied for credit cards from Capital One." (*Id.* at 4.) Additionally, the superseding indictment alleges that Ms. Thompson used the obtained security credentials to use the computing power of the AWS servers rented by certain victim AWS customers to mine cryptocurrency, attempted to use PII taken from Capital One's servers to create unauthorized credit and debit cards, and intentionally and unlawfully possessed the PII of Capital One customers. (*Id.* at 5, 7-9.) As to Counts 2 through 5, the superseding indictment claims that the value of the information obtained by Ms. Thompson exceeded $5,000. (*Id.* at 6-8.) For Counts 6 and 7, the value of the information is not alleged. (*Id.* at 7.) For Count 8, the Indictment alleges that Ms. Thompson's alleged cryptocurrency mining cost certain entities a loss of over $5,000. (*Id.* at 7-8.) To sustain its burden of proof on charges in the superseding indictment, the government must establish beyond a reasonable doubt, among other things, a

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

scheme or artifice to defraud, Ms. Thompson's specific intent[3] to defraud, and that she intentionally accessed a computer without authorization and thereby obtained financial and/or protected information. *See, e.g.*, *United States v. Jinian*, 725 F.3d 954, 960 (9th Cir. 2013) (wire fraud); *United States v. Manion*, 339 F.3d 1153, 1156 (9th Cir. 2003) (wire fraud); 18 U.S.C. §§ 1030(a)(2)(A) and (C) (CFAA); *United States v. Suphunthuchat,* 400 F. App'x 182, 183 (9th Cir. 2010) (access device fraud); *Flores-Figueroa v. United States*, 556 U.S. 646, 647 (2009) (aggravated identity theft). Because the government has also charged Ms. Thompson with a violation of 18 U.S.C. § 1030(c)(2)(B)(iii), it must also prove beyond a reasonable doubt that the value of the information Ms. Thompson allegedly obtained exceeded $5,000.

On February 19, 2021, pursuant to Rule 17(c), the defense issued a trial subpoena to AWS that requested nine categories of documents. Following service of the subpoena, counsel for both AWS and Ms. Thompson met and conferred on numerous occasions and reached agreement on many issues, including a protective order. This meet and confer process also led to the issuance of an updated subpoena to AWS dated November 24, 2021. (See 11/24/21 Subpoena and Attach. A, attached hereto as Exhibit A.) As a result of the meet and confer process, AWS voluntarily agreed to produce certain documents and information responsive to seven of the nine outstanding subpoena requests.[4] In those cases, counsel for AWS has let the defense know that once the protective order is signed by the Court, it hopes to produce materials within a week or so.[5]

[3] The government's burden is high: they must prove Ms. Thompson had a specific "intent to deceive and cheat." *United States v. Miller*, 953 F.3d 1095, 1103 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1085, 208 L. Ed. 2d 539 (2021).

[4] For example, AWS has agreed to provide Office of Chief Information Security Office ("CISO")-related communications, but not those of other Executive Officers unless they are with the CISO.

[5] Ms. Thompson, of course, reserves her right to seek additional documents and communications from AWS, and nothing in this motion is intended to waive any of her rights.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

That said, as of the date of the filing of this motion, there remain two categories of documents in the subpoena that AWS has stated it will not produce. The outstanding requests are:

> **Request No. 8**
>
> Any contracts relating to cloud infrastructure and/or WAFs between the Company and one of the following parties: Capital One, [Victim 2], [Victim 3], [Victim 4, [Victim 5], [Victim 6], [Victim 7], and/or [Victim 8].
>
> **Request No. 9**
>
> Any bills and invoices for providing cloud infrastructure from January 1, 2019 through December 31, 2020 sent from the Company to the following entities: AWS, Capital One, [Victim 2], [Victim 3], [Victim 4], [Victim 5], [Victim 6],[Victim 7], and/or [Victim 8].

(Exh. A.) Before filing this motion, counsel for Ms. Thompson conferred telephonically with counsel for AWS regarding the basis for this motion and the two requests in dispute. (12/6/21 Ltr. from T. Newby to B. Klein, attached as Exh. B.) Regarding Subpoena Requests Nos. 8 and 9, AWS is not willing to produce any documents absent a court order.

AWS has requested until January 14, 2022 to oppose this motion. Ms. Thompson consents to that request.

III. ARGUMENT

The Court should order AWS to produce documents responsive to Subpoena Requests No. 8-9 (the "Requests") no later than seven days after the Court's entry of order in this matter to ensure that Ms. Thompson has the materials sufficiently in advance of trial. The facts and circumstances of this case, as well as the law support such an order.

Given the nature of the pending charges against Ms. Thompson, the alleged "misconfigurations" of the AWS servers rented by the alleged victim entities, most

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

notably Capital One, are central to Ms. Thompson's defense as those "misconfigurations" go directly to whether she accessed a computer without authorization, as well as to her specific intent. The alleged "value" of the information obtained, as well as any monetary "loss" to the alleged victims due to Ms. Thompson's alleged exploitation of the "misconfigurations" is also directly relevant to the wire fraud and computer fraud and abuse charges.[6] These are precisely the kind of materials Rule 17(c) was intended to facilitate production of in advance of trial.

Rule 17 broadly allows defendants to subpoena third-party information and "is substantially the same as rule 45(a)" of the Civil Rules. See Fed. R. Crim. P. 17, adv. comm. n. 1944. While Rule 17 is not a discovery tool, in criminal cases, many district courts interpret the rule liberally. A liberal interpretation makes sense given the bizarre dichotomy between civil cases, where parties fighting over money have immense discovery powers, and criminal cases, where a defendant fighting for her liberty has virtually no discovery powers: "It is ironic that a defendant in a breach of contract case" can "compel third-parties to produce any documents" that reasonably lead to discoverable evidence, while a "defendant on trial for his life or liberty does not even have the right to obtain documents 'material to his defense' from those same third-parties." *United States v. Nosal*, 291 F.R.D. 403, 408 (N.D. Cal. 2013) (quoting United *States v. Rajaratnam*, 753 F. Supp. 2d 317, 320 (S.D.N.Y. 2011) (citation omitted)); see *United States v. Tomison*, 969 F. Supp. 587, 593 n. 14 (E.D. Cal. 1997) (Rule 17(c) "may well be a proper device for discovering documents in the hands of third parties" and the full restrictions on Rule 17 "only apply to documents in the government's

[6] The documents sought are also highly relevant to sentencing, should Ms. Thompson proceed to that phase of the case. *See, e.g.,* USSG § 2B1.1(b)(1) (applying guidelines level increases for amount of loss); *id.* at (b)(10) (enhancement for "sophisticated means"); *id.* at (b)(11) (enhancement for use of an "authentication feature"); *id.* at (b)(17) (enhancement for "jeopardiz[ing] the safety and soundness of a financial institution"); *id.* at (b)(18) (enhancement for "intent to obtain personal information").

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

hands"); *United States v. Nixon,* 418 U.S. 683, 700 n.12 (1974) (reserving the issue of whether the restriction on discovery applies "in its full vigor when the subpoena duces tecum is issued to third parties rather than government prosecutors").

Rule17(c) authorizes courts to direct a party to produce materials designated in a subpoena before trial in order "to facilitate and expedite trials." *United States v. Carter*, 15 F.R.D. 367, 369 (D.D.C. 1954). Indeed, the "chief innovation" of Rule 17(c) was "to expedite the trial by providing a time and place before trial for the inspection of subpoenaed material." *Nixon*, 418 U.S. at 698-9 (citing *Bowman Dairy Co. v. United States,* 341 U.S. 214, 220 (1951)); *see also United States v. Gosar*, Nos. 19-306, 19-307-, 19-308, 19-313, 19-315, 19-320, 2020 WL 263613, at *1 (W.D. Wash. Jan. 17, 2020). To substantiate the early return of a trial subpoena, the moving party must clear "three hurdles:" (1) relevancy; (2) admissibility; and (3) specificity. *Nixon,* 418 U.S. at 700; *see Gosar*, 2020 WL 263613, at *2.

Additionally, a court must consider whether the materials sought are "otherwise procurable reasonably in advance of trial by exercise of due diligence;" whether a defendant, like Ms. Thompson, can "properly prepare for trial without such production and inspection in advance of trial;" whether the "failure to obtain such inspection may tend unreasonably to delay the trial;" and whether the "application is made in good faith and is not intended as a general 'fishing expedition.'" *United States v. Krane*, 625 F.3d 568, 574 (9th Cir. 2010) (quoting *Nixon*, 418 U.S. at 699-700); see also *Gosar*, 2020 WL 263613, at *2. Ms. Thompson's request for the early return of materials from AWS easily meets those requirements.

/ /

/ /

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

A. The Documents Sought from AWS are Relevant, Admissible, and Described with the Requisite Particularity.

To establish relevancy, admissibility, and specificity, Ms. Thompson need only demonstrate a "sufficient likelihood," demonstrated through rational inferences that the documents sought "relate to the offenses charged in the indictment." *United States v. Pacific Gas and Electric Co.*, No. 14CR00175THE1MEJ, 2016 WL 1212091, at *5 (N.D. Cal. Mar. 28, 2016); see *Nixon*, 418 U.S. at 700; *Bowman Dairy*, 341 U.S. at 219-20 (stating that it is sufficient if the subpoenaed material "could be used at trial"). The material requested in the Requests meets this standard.

The Requests are both specific and limited in temporal and categorical scope. Further, they are clearly relevant to the charges in the indictment. Ms. Thompson's "intent" is paramount to the charges levied against her by the government. The discovery produced to date indicates that Capital One, in its communications with AWS, initially referred to Ms. Thompson as a "researcher." It goes without saying that a person who accesses a firewall "misconfiguration" as a "researcher" has a far different intent than one who does so as a "hacker."

Turning now to the first disputed request, Request No. 8, the contracts between AWS and the alleged victim entities relating to cloud infrastructure will help explain, exactly, what kind of cloud infrastructure the alleged victims were renting from AWS and will inform Ms. Thompson, potentially, about any limitations or configuration weaknesses about which AWS advised the victim entities from initiation of the relationship between the two parties. It may also shed light on whether the alleged victim entities, including Capital One, contemplated any type of "value" associated with the data stored on AWS servers. As for Request No. 9, the request for bills and invoices is directly relevant and admissible to the government's allegations of "cryptojacking" and concomitant "damage" to the victim entities. The government has

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

alleged over $5,000 in damages from Ms. Thompson's alleged "cryptojacking," but produced no evidence of *any* damage. Ms. Thompson should thus be able to see for herself whether the alleged mining caused any sort of "damage" to any of the alleged victim entities' wallets. The discovery sought by the Requests is not only relevant and admissible as to Ms. Thompson's defense of the government's charges, but it is also relevant and admissible as impeachment evidence of any witnesses called by the government, including government witnesses and witnesses from AWS, Capital One, and the other victim entities.

B. The Defense Requires the Requested Materials in Advance of Trial and Cannot Obtain the Material Through Other Means.

At present, there are no other means for Ms. Thompson to obtain the material requested but directly from AWS—the materials requested are not in the government's discovery to date and are not in any way publicly accessible to Ms. Thompson.[7] The materials are also needed in advance of trial because they are necessary for Ms. Thompson's expert(s) to review in preparation for her defense. If the materials were not provided in advance of trial, then it is likely that the trial would need to be delayed so that Ms. Thompson's defense team and experts could properly absorb the materials in the midst of trial. See *Nixon*, 418 U.S. at 702 (stating that a pre-trial return of materials is appropriate where the materials have "valid potential evidentiary uses" and analysis "may take a significant period of time"); *Pacific Gas*, 2016 WL 1212091, at *6 (noting that pre-trial return of "impeachment" materials is warranted when those same

[7] Ms. Thompson has also issued third-party subpoenas to Capital One and the Office of the Comptroller of the Currency ("OCC"). To date, Capital One has refused to produce documents relevant to similar requests, which is subject to separate motion practice for early return. (*See* Dkts. Nos. 111, 112, 118, 119, 121.) In any event, Capital One's materials would not include contracts and invoices relevant to the other alleged victim entities. It is unknown whether the OCC is in possession of documents relevant to these same requests; to date, it has refused to produce any documents to Ms. Thompson.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

materials have other "valid potential evidentiary uses"). Thus, pretrial return of the materials requested from AWS is appropriate and warranted.

C. The Subpoena is Neither Unreasonable Nor Oppressive.

Rule 17 subpoenas "may be quashed if their production would be 'unreasonable or oppressive,' but not otherwise." *Nixon*, 418 U.S. at 698. A Rule 17(c) subpoena, like this one, can be quashed as "unreasonable or oppressive" if it calls for privileged matter. *See Gosar*, 2020 WL 263613, at *2; *Pacific Gas*, 2016 WL 1212091, at *3. Here, the Requests are not unreasonable in their scope, which is appropriately and specifically limited both in time and in subject matter.

II. CONCLUSION

For the above stated reasons, Ms. Thompson respectfully requests that the Court grant this motion and order Capital One to produce the materials no later than 7 days after the Court's entry of the proposed order.

DATED: January 4, 2022.

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI

/s/ Christopher Sanders
CHRISTOPHER SANDERS

/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

/s/ Brian Klein
BRIAN KLEIN

/s/ Melissa Meister
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100